BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
	)	CG Docket No. 17-59
Advanced Methods to Target and Eliminate	)	
Unlawful Robocalls	)	FCC 17-24
	)	

Comments of Professional Association for Customer Engagement

Filed July 3, 2017

Stuart Discount
Professional Association for
Customer Engagement
8445 Keystone Crossing, Suite 106
Indianapolis, Indiana 46240

Chairperson of Professional Association for Customer Engagement

Michele A. Shuster, Esq.
Nicholas R. Whisler, Esq.
Joshua O. Stevens, Esq.
Mac Murray & Shuster LLP
6530 West Campus Oval, Suite 210
New Albany, Ohio 43054

Counsel for Professional Association for Customer Engagement

I. Introduction

The Professional Association for Customer Engagement ("PACE")[1] respectfully submits these Comments in response to the Federal Communications Commission's ("FCC" or "Commission") above-cited Notice of Proposed Rulemaking and Notice of Inquiry ("NPRM/NOI") regarding the imposition of rules allowing carriers to refuse or "block" calls from telephone numbers in various circumstances. PACE recognizes the need to combat illegal robocalls[2] and supports efforts to identify and prosecute bad actors. However, PACE is also concerned about empowering carriers to refuse to carry traffic or originate calls from legitimate and legal businesses. To that end, PACE urges the FCC to limit legal blocking to only calls purporting to originate from (1) numbers requested to be blocked by their subscribers, (2) invalid numbers, (3) numbers not allocated to any carrier, and (4) a carrier's own unassigned numbers. At this time, due to the lack of a central database of allocated but unassigned numbers and the anticompetitive risks of such a database, PACE requests that the FCC not consider mandating blocking of calls purporting to originate from allocated but unassigned numbers. Lastly, because of the possibility of anticompetitive behavior as a result of allowing carriers to block "presumptively illegal" calls, even when utilizing the recently developed SHAKEN & STIR[3] authentication protocols as a basis for the presumption, PACE strongly opposes permitting carriers to block calls under a "presumptively illegal" standard.

[1] PACE is the only non-profit trade organization dedicated exclusively to the advancement of companies that use a multi-channel approach to engaging their customers, both business-to-business and business-to-consumer. These channels include contact centers, email, chat, social media, web and text. Our membership is made up of Fortune 500 companies, contact centers, BPO's, economic development organizations and technology suppliers that enable companies to contact or enhance contact with their customers.

[2] The term "robocall" has various meanings in the industry and within the FCC. Compare, e.g., the FCC's July 2015 Order (FCC-72, Fn. 1) defining the term with paragraph 13 of the NPRM/NOI. As used herein, "robocall" refers to a prerecorded message. Prerecorded messages are often used for legitimate and legal purposes such as to provide prescription refill reminders or delivery notifications; however, bad actors use prerecorded messages to scam and harass consumers in violation of laws.

[3] Signature-based Handling of Asserted information using toKENs ("SHAKEN") and Secure Telephony Identity Revisited ("STIR"). Although noted as "recently developed", the industry associations and working groups responsible for SHAKEN & STIR continue to make refinements as they work toward implementation of the protocols.

II. Background

A. Illegal Robocall Problem

Unwanted calls, including those involving scams and illegal telemarketing solicitations, are the number one complaint received by the FCC.[4] In its 2015 Declaratory Ruling and Order, the Commission stated on the issue of robocall blocking, "nothing in the Communications Act or our rules or orders prohibits carriers or voice over internet protocol ("VoIP") providers from implementing call-blocking technology that can help consumers who choose to use such technology to stop unwanted robocalls."[5] The FCC also convened a Robocall Strike Force on August 19, 2016 comprised of various telecommunication stakeholders in an attempt to find a solution to the illegal robocall problem and, specifically, illegal operators "spoofing" telephone numbers to avoid identification and accountability.[6]

At a high level, under current VoIP standards, a "call" is in reality two components: a voice data stream and an informational data packet carrying call information (e.g., originating number, terminating number).[7] When a caller originates a call from an IP address, that caller may indicate in the informational data packet a different calling party number than the "true" originating number of the call. Legitimate business reasons exist to support this functionality. For example, a business that operates from multiple offices around the country may want the caller ID to display a single inbound customer service number regardless of the office originating the outbound call.

---

[4] *See* Tom Wheeler, *Cutting Off Robocalls*, FCC (Jul. 22, 2016) https://www.fcc.gov/news-events/blog/2016/07/22/cutting-robocalls.

[5] *See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Declaratory Ruling and Order, CG Docket No. 02-278, WC Docket No. 07-135, FCC 15-72, ¶ 152 (Jul. 10, 2015).

[6] Robocall Strike Force participant AT&T published a list of initial corporate members. *FCC Hosts First Robocall Strike Force Meeting; AT&T's Stephensen to Chair Industry-Led Group*, AT&T (Aug. 19, 2016) https://www.attpublicpolicy.com/fcc/fcc-hosts-first-robocall-strike-force-meeting-atts-stephenson-to-chair-industry-led-group/.

[7] The history of VoIP deployment provides additional context. Before VoIP, businesses and contact centers operated using time division multiplexing ("TDM") systems. After the FTC instituted its Do Not Call rules requiring contact centers to display the number of the party on whose behalf they are calling, contact centers began switching from T1 lines using TDM to Primary Rate Interface ("PRI") systems. PRI allows the caller to indicate caller ID information. Subsequently, VoIP systems began to be adopted by businesses and contact centers due to their lower cost. VoIP also allows indication of caller ID information, but unlike PRI, which uses a physical circuit delivered to the business' address, VoIP uses the public internet associated with an IP address. Because VoIP uses a virtual connection instead of a physical circuit, identification of a VoIP user is very difficult.

Additionally, a contact center calling on behalf of a client may want or need to provide the client's telephone number for return calls. Such legitimate uses are actually helpful for consumers.

Yet, as with any technology, unscrupulous actors found a way to exploit the caller ID feature. Individuals originating calls with the intent to defraud (as defined in the Truth in Caller ID Act),[8] often located in foreign countries, will use this feature to "spoof" the telephone number or calling party name of a third-party to trick consumers. The use of VoIP technology means that tracing the call originator is difficult, and hence these unscrupulous actors can evade authorities.[9] One common scam involves the caller pretending to be the Internal Revenue Service ("IRS") seeking payment for past due taxes and fines.[10] Spoofing is also used by unscrupulous telemarketers to hide their true identity as they avoid complying with state and federal do-not-call lists and registration requirements. But because, at its core, the technology exploited by scammers is also a legitimate tool for businesses, any regulation of spoofing is difficult to achieve without impacting legitimate business communications.

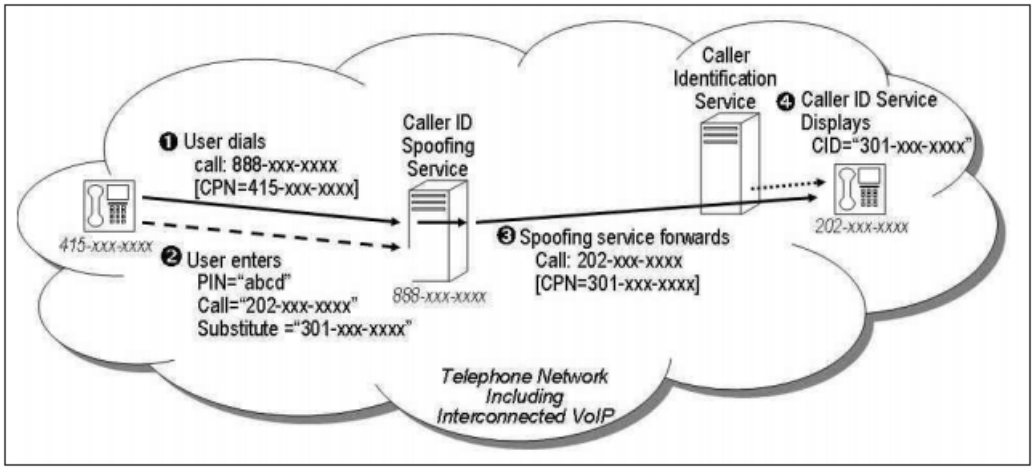

Figure 1: Depiction of caller ID Spoofing.[11]

[8] 47 U.S.C. § 227(e)(1) ("It shall be unlawful for any person within the United States, in connection with any telecommunications service or IP-enabled voice service, to cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value . . .").

[9] *See* Bikram Bandy, *Your Top 5 Questions About Unwanted Calls and the National Do Not Call Registry*, FED. TRADE COMM. (Mar. 8, 2015), https://www.consumer.ftc.gov/blog/your-top-5-questions-about-unwanted-calls-and-national-do-not-call-registry.

[10] *See Scam Phone Calls Continue; IRS Identifies Five Easy Ways to Spot Suspicious Calls*, INTERNAL REVENUE SERV. (Aug. 28, 2014), https://www.irs.gov/uac/newsroom/scam-phone-calls-continue-irs-identifies-five-easy-ways-to-spot-suspicious-calls.

[11] *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, Declaratory Ruling and Order, WC Docket No. 11-39, FCC 11-100, ¶ 16, Fig. 1 (Jun. 22, 2011).

Presently, telecommunication service providers face immense challenges when attempting to ascertain whether the calling party number received for an incoming call at a VoIP gateway is the correct calling party number.[12] Further, the current VoIP standard does not allow law enforcement or regulatory agencies to easily trace back calls to their originators using caller ID information. Without effective trace back tools, law enforcement and industry are at a loss to stop the flood of scam calls harassing consumers every day. Industry consensus exists for a long-term solution utilizing mechanisms to validate the authenticity of the calling party and assist law enforcement in tracing back illegal robocalls to their source. PACE supports such efforts to effectively identify and prosecute bad actors.

III. FCC's Proposed Solution

The Commission's NPRM/NOI focuses on one possible method of reducing illegal robocalls, namely, allowing carriers to block calls passing over their networks based on certain characteristics. PACE believes that any solution, including the one proposed by the Commission in its NRPM/NOI, must comport with several principles. First, the solution must reduce the ability of illegal robocalls to reach consumers. Second, the solution must not prevent or block legal communications. Third, the solution should allow consumers to choose how they want to manage their communications. Fourth, the solution should work for both wireless and wireline consumers. Fifth, the solution should make it easier for law enforcement to identify and prosecute offenders. Whether short-term or long-term, the solution should focus on effectively eliminating illegal robocalls with as little disruption as possible to legal and wanted communications that facilitate commerce. However, there is a benefit to avoiding deploying multiple solutions (i.e., both a long-term and short-term solution) and hence greater consideration should be given to a long term solution.

Call blocking rules, while arguably an effective solution for blocking calls originating from numbers requested to be blocked by subscribers and invalid or unallocated numbers, pose a high risk of being used to block legitimate communications if applied to presumptively illegal calls using ill-defined standards. However, a solution for blocking these types of illegal calls may not be effective against other types of illegal, spoofed calls. Additionally, as will be explained more fully below, allowing carriers to determine whether a communication is presumptively illegal

[12] *See CallerID*, VOIP-INFO.ORG (May 28, 2011), http://www.voip-info.org/wiki/view/CallerID.

raises the specter of anticompetitive behavior on the part of carriers and harm to businesses that rely on multiple carriers for day-to-day operations. Any call blocking the Commission chooses to permit should be limited in scope and targeted to reduce calls from bad actors, not legitimate businesses.

A. Carrier Call Blocking and Category-Based Blocking

The Commission's NPRM/NOI proposes allowing carriers to block calls in four circumstances based on the caller ID information transmitted with the call: (1) calls originating from a number designated for blocking by its subscriber, (2) invalid numbers, (3) unallocated numbers, and (4) allocated but unassigned numbers.

i. Subscriber Requested

PACE supports allowing carriers to block calls using a calling party number where the subscriber of that number has designated that number to block. Usage of the calling party number would be, in effect, unauthorized usage. Like with the IRS scam, where the number displayed to the consumer was an inbound-only number for the IRS, many businesses have publicly-listed inbound numbers from which they do not originate calls. If the subscriber designates that such a number would never originate a call, then carriers should be allowed to block calls purporting to originate from that number. Such calls would represent unauthorized spoofing of that number.

ii. Invalid Numbers

PACE further supports allowing carriers to block calls purporting to originate from an invalid number (e.g. too few digits, single digit repeated, N11 code in place of area code, unassigned area code). Because invalid numbers would never be able to ring back to a caller, there is no legitimate business need to display such numbers. Therefore, there is little to no risk of blocking legitimate calls by blocking invalid number calls.

iii. Unallocated Numbers

PACE also supports allowing carriers to block calls purporting to originate from a number that has not been allocated to a carrier by the North American Numbering Plan Administrator ("NANPA"). However, at this time, PACE does not support mandating such a capability nor mandating any particular infrastructure solution for implementing this capability.

iv. Unassigned Numbers

At this time, PACE requests that the Commission not mandate a carrier block calls purporting to originate from a number that has been allocated to another carrier but not assigned

to a subscriber of that other carrier. First, no carrier-accessible database currently exists for determining whether an allocated number has been assigned to a subscriber. Because number assignment is internal to the assigning provider, such information is not public. Second, no central database of assigned numbers should be created as it would convert what is currently proprietary trade secret information for many carriers (subscriber counts, trends in subscriber assignment) into effectively public information. This would harm carriers by exposing their internal statistics to their competitors. Third, even if the database could be held by a neutral third-party and the data sufficiently anonymized, reporting to such a database would be burdensome to small carriers who may not be able to readily absorb the implementation and ongoing costs of such a reporting obligation. Consequently, at this time, PACE does not support mandating such a capability, nor mandating any particular infrastructure for implementing this capability.

B. "Presumptively Illegal" Calls

The NPRM/NOI also discusses allowing carriers to block "presumptively illegal" calls using carrier-developed standards. The FCC should not adopt presumptively illegal call blocking. Access to the telephone network is an essential component of a well-functioning economy and the free flow of information in today's society. Permitting carriers to regulate who has access to the telephone network, or the degree of access available, based on an imprecise system of presumptions would present a high risk of silencing unpopular speakers, blocking consumer access to important but high volume information, and opening the door for carriers to use their presumptions to block traffic from disfavored carriers across their networks. No matter the standards used to determine whether a call is presumptively illegal, the potential for abuse far outweighs any benefit to be gained. The determination of whether calls are illegal or not should be left to judiciary, regulatory, and law enforcement bodies, and carriers should not be tasked with, nor given, such authority.

C. SHAKEN & STIR

One potential solution touted by the Commission is implementing the SHAKEN & STIR authentication protocols.[13] Generally speaking, SHAKEN & STIR allows a VoIP call and its associated telephone number to be authoritatively and cryptographically signed by the originating

[13] *NPRM/NOI at ¶ 32.*

carrier.[14] The originating carrier also assigns an attestation rating of full attestation, partial attestation or gateway attestation (only attesting to point of entry). When the terminating service provider receives the call and number information, it uses a public decryption key to verify the information. Using the attestation rating, the terminating carrier may also elect to block the call or provide a call designation (e.g., verified, likely spam) to the call recipient.

The SHAKEN & STIR protocols are an admirable first step to reducing the incentive for spoofers to engage in harmful activities, but, at this time, they are not sufficiently developed to rely upon as a basis for call blocking or call designation. For example, many large businesses use multiple carriers for redundancy and/or to obtain efficiencies in call routing. Often such businesses will purchase phone numbers from a single carrier or a carrier that is not the one on which the call will be carried. Under SHAKEN & STIR, a full attestation is only available if the business places a call using the same carrier as the carrier from which it purchased the phone number associated with the call. If the carriers differ, then only a partial attestation will be provided. Carriers could decide to block or designate as potentially fraudulent calls with only partial attestation even though the calls are entirely legitimate. Businesses, as a result, would be forced to give up redundant systems and cost efficiencies in order to obtain a full attestation.

A simple example will help illustrate how this attestation difficulty could work in the real world. A hypothetical school district uses two carriers to support its telecommunications needs: Carrier 1 and Carrier 2. Carrier 1 is the primary carrier for the school district and all phone numbers used by the district were purchased from Carrier 1. Carrier 2 is a backup in the event Carrier 1 experiences technical difficulties or rapid message deployment is needed using both carriers. One day a major storm front develops unexpectedly that is predicted to cause rapid flash flooding. The district determines that it needs to release students early for their safety and implements its emergency communications plan which includes initiating prerecorded message calls to parents using both carriers. Because all phone numbers were purchased from Carrier 1, Carrier 1 is able to fully attest all calls originating on its network. However, Carrier 2 is only able to partially attest the calls originating on its network because they use a phone number purchased from Carrier 1. Terminating carriers, identifying the Carrier 2 calls as only partially attested, flag

[14] *Robocall Strike Force Report (Oct. 26, 2016)* at 5 (available at https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf).

them as potential spam and block them from parents. Many parents do not receive the calls and the district struggles to efficiently send students home before the storms arrive.

In order to prevent this type of two-tier communication system where carriers only fully attest their own phone numbers, the Commission must implement clear rules mandating SHAKEN & STIR interoperability between carriers regardless of size. One mechanism to achieve this goal is requiring that the originating carrier provide full attestation when a call originates from an IP address and phone number combination matching client-registered combinations regardless of the carrier from which the phone number was purchased. Alternatively, the Commission could direct the implementation of a hierarchical information database of legitimate IP address and phone number combinations populated by carriers based on client registrations, similar to a DNS registry. Likewise, the Commission could order carriers issuing phone numbers to keep up-to-date tables of the IP addresses from which legitimate calls using each phone number will originate. Call transmission information could then include an identifier allowing the terminating carrier to identify the correct carrier database to validate the sending IP address similar to the Sender Policy Framework used in e-mail communications.

The development of SHAKEN & STIR, and its ability to trace back illegal calls, holds out promise that the mere ability to quickly and accurately traceback a call will drastically reduce the number of illegal calls occurring. Thus, it is possible that the deployment of SHAKEN & STIR may reduce the need for other short term infrastructure solutions. Nevertheless, PACE cannot understate the importance of ensuring a level playing field for telephone communications. Before SHAKEN & STIR is implemented, the FCC must take steps to prevent carriers from blocking or negatively designating calls made using a different carrier's phone number. Without such regulations, businesses will be forced to abandon multi-carrier redundancy or cost-efficient routing because calls made with numbers purchased from the non-originating carrier will only be capable of partial attestation.

IV. Conclusion

For the foregoing reasons, the Commission should only permit carriers to block calls purporting to originate from (1) numbers requested to be blocked by their subscribers, (2) invalid numbers, (3) numbers not allocated to any carrier, and (4) a carrier's own unassigned numbers. At this time, due to the lack of a central database of allocated for unassigned numbers and the anticompetitive risks and burdensome costs of such a database to small carriers, PACE requests

that the FCC not mandate blocking of calls purporting to originate from allocated but unassigned numbers on an inter-carrier basis, nor the infrastructure for doing so. Lastly, because of the high probability of anticompetitive behavior as a result of allowing carriers to block presumptively illegal calls, even when utilizing the recently developed SHAKEN & STIR authentication protocols as a basis for the presumption, PACE is strongly opposed to permitting carriers to block calls under a presumptively illegal standard.

Respectfully submitted,

/s/ Michele A. Shuster
Michele A. Shuster, Esq.
Nicholas R. Whisler, Esq.
Joshua O. Stevens, Esq.
Mac Murray & Shuster LLP
6530 West Campus Oval, Suite 210
New Albany, OH 43054
Telephone: (614) 939-9955
Facsimile: (614) 939-9954

Counsel for Professional Association for Customer Engagement